PATENT

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Inventor: James T. Lynn et al.	)	Confirmation No.: 3710
	)	
	)	Customer No.: 000043471
U.S. Serial No.: 09/814,601	)	
	)	Art Unit: 2137
Filed: March 23, 2001	)	
	)	Examiner: Zachary A. Davis
	)	

Title: SECURING DISTRIBUTING SOFTWARE COMPONETS ON A NETWORK

PRE-APPEAL BRIEF
REQUEST FOR REVIEW

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir,

Please enter these arguments in response to the Final Office Action mailed on May 26, 2006 and conduct a pre-appeal brief conference. Applicant respectfully requests withdrawal of the outstanding rejection.

REMARKS

I. Introduction

Claims 1-5 are pending in the above application.

Claims 1-5 stand rejected under 35 U.S.C. § 102(e).

Claim 1 is the only independent claim.

II. Slivka Does Not Disclose Applicant's Claimed Invention

Claims 1-5 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Slivka et al. (U.S. Pat. No. 6,049,671) (hereafter "Slivka"). Applicant respectfully traverses this rejection.

As explained on the first page of Applicant's disclosure, one of the functions of an operating system (OS) which resides on a network appliance (e.g., personal computer, set-top box, satellite dish) is to download software updates in the form of components or plug-in modules over the network. Network users download upgrades, plug-ins, programs and applications from various sources, such as Internet websites, cable-based service providers, CD ROMs, and the like. Although a number of security mechanisms are available to these service providers, hosts and end users, it remains problematic to ensure that the downloaded module has not been tampered with or otherwise modified from its original form. Similarly, despite presently known security mechanisms, it is difficult for distributors to ensure that only authorized end users receive the distributed modules. Applicant's invention addresses these problems.

The applied prior art of Slivka does not acknowledge these problems, and at best merely discloses a system which enables conventional network downloads in which these problems arise. For example, while the present invention would consider a network element with unknown software on it a security risk which would inhibit loading of additional software on it (Fig. 1, element 110), Slivka is more than happy to sell such network element another software program or to update existing known programs on the network element. See, Slivka, col. 7: 64 through col. 8: 5 ("the user computer may also contain software that is not known by the update service … this computer software is marked 'unknown' … [a]fter the service update application complete the analysis of user computer software, a summary report is sent back to the user computer"). Slivka is not concerned whether or not the network element itself is authorized to operate a program, Slivka simply provides an on-line "store" to allow a user to pick and choose any program desired. As discussed in detail below, Slivka simply does not anticipate

Applicant's claimed invention.

Anticipation under 35 U.S.C. § 102 requires that each and every element of the claim be disclosed in a prior art reference as arranged in the claim. See, *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1380 (Fed. Cir. June 2006) ("a claim is anticipated under 35 U.S.C. § 102 'if each and every limitation is found either expressly or inherently in a single prior art reference'" citing, *Bristol-Myers Squibb Co. v. Ben Venue Labs, Inc.*, 246 F.3d 1368, 1374 (Fed. Cir. 2001). See also, *Akzo N.V. v. U.S. Int'l Trade Commission*, 808 F.2d 1471 (Fed. Cir. 1986); *Connell v. Sears, Roebuck & Co.*, 220 USPQ 193, 198 (Fed. Cir. 1983).

Slivka does not disclose or suggest a method for securely distributing a component from a network host to a network appliance, which includes the steps of: signing, by said network host, a configuration file including a load table which defines a plurality of authorized components for said network appliance; executing a secure kernel and said signed configuration file on said network appliance, said secure kernel including computer code for checking the authenticity of said configuration file and boot code for allowing said network appliance to initially boot up and establish communication with said network host; verifying, by said secure kernel, the authenticity of said configuration file; reading, by said secure kernel, said load table only after said verifying step; and loading said plurality of authorized components defined in said load table onto said network appliance, as recited by claim 1.

Slivka merely discloses a method of providing programs, updates and patches of programs from an update service to a user's computer, i.e. Slivka is nothing more than an on-line store and support service provider. Abs.; Figs. 4A and 4B, element 86 ("user chooses which computer software to download"); col. 5: 47 through col. 6: 56. Slivka does not disclose a signed configuration file including a load table which defines a plurality of authorized components for said network appliance, as recited by claim 1. While the Examiner clarifies in the Advisory Action that Slivka's disclosed "cabinet file" (which is later placed in a distribution file which may be digitally signed) is being applied against Applicant's claimed "configuration file" and directs Applicant to col. 8: 34-42 and col. 16: 55 through col. 18: 15, the Examiner is respectfully mistaken. Slivka explains that the "cabinet file" is created to transfer a selected program or update (a.k.a. download) to a user such as by compressing the selected program, providing appropriate packaging for a secure transfer (e.g. SSD), and adding an installation program (e.g. "self-extracting archive of files") to make the downloaded program self extracting when received by the user's computer. Slivka, Fig. 7, element 132; col. 4: 6-7 "Fig. 7 is a flow diagram illustrating a method of obtaining software over a computer network"; col. 13: 6-68 ("the file of directive commands … is used to create a Cabinet file"); col. 17: 51 through col. 18: 60. Column 8 of Slivka merely discloses to provide a menu of available programs, including new programs, and updates that the user may want to download.

There is no suggestion to include the menu of available programs, new programs and updates discussed in column 8 of Slivka in a cabinet file, as the Examiner concludes. As a practical matter, it would hardly be desirable or beneficial to encrypt a listing of programs to prevent viewing by the public at large when one is trying to sell such programs to the public at large. Moreover, while Slivka clearly discloses to install the program in the cabinet file on a user's computer (Slivka, col. 18: 35-60), a listing of programs and updates available for downloading, which is likely to frequently change, clearly would not be beneficial or desirable to have installed on a user's computer.

Finally, Slivka makes it very clear that the purchased program can be downloaded to any network element, including ones with "unknown" software. Slivka, col. 7: 66 through col. 8: 5.

As Slivka discloses that "unknown" programs may exist on a user's computer, the cabinet file clearly cannot contain these unknown programs in a list of "authorized components for said network appliance" as required by the "load table" in Applicant's claim 1.

In summary, Slivka simply does not disclose to sign a configuration file including a load table which defines a plurality of authorized components for said network appliance, as recited by Applicant's claims. Accordingly, as Slivka does not disclose each and every element of the claims, as set forth in the claims, Slivka does not anticipate the above claims.

III. Conclusion

Having fully responded to the Office action, the application is believed to be in condition for allowance. Should any issues arise that prevent early allowance of the above application, the examiner is invited contact the undersigned to resolve such issues.

To the extent an extension of time is needed for consideration of this response, Applicant hereby request such extension and, the Commissioner is hereby authorized to charge deposit account number 502117 for any fees associated therewith.

Respectfully submitted,

By: /Lawrence T. Cullen/
Lawrence T. Cullen
Reg. No.: 44,489

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1797